REMARKS

In view of the above amendment, applicant believes the pending application is in condition for allowance.

The Office Action and prior art relied upon have been carefully considered. Claim 6 was rejected under 35 U.S.C. § 102(b) as being anticipated by Kim (US 5,796,837). Claims 1-3, 9-11 and 27-29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kim in view the Langford publication. Claims 8, 13, 14-16, 18-23, 25, 26 and 31-38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kim in view of the Jakobsen publication.

In an effort to expedite the prosecution Claims 1, 3, 9, 11, 27, 29, 33-38 have been cancelled. Claims 6, 13 and 20 have been amended to emphasize the difference of applicant's S-box as compared to that of the Kim patent.

The present invention as well as the cited Kim patent are directed to the generation of S-boxes that are resistant to various types of cryptanalysis.

With respect of claim 6, applicant reiterates its position as stated in the previous response, namely, that the Examiner has overlooked the feature that the candidate function generating means generates candidate functions, each formed by a composite function composed of two functions of different algebraic structures. This feature is based on the inventor's finding described from page 17, line 27 to page 19, line 22, and is not taught or suggested by Kim.

In this connection, the Examiner refers, in the last paragraph of item 12, to various sections of column 4 of Kim. However, the mentioned sections deal with: (1) the process for checking whether the S-box satisfies the condition D1 related to the

differential cryptanalysis (col. 4, lines 10-11); and (2) conditions L1 to L5 related to the linear cryptanalysis (col. 4, lines 31, 41, 51, 63). The Kim patent discloses nothing about forming an S-box by a composite function composed of two functions of different algebraic structures.

An example of the S-box according to the Kim patent is shown as a random number table in Fig. 5, where two out of six input bits (see Fig. 4) are used to select one of the four rows, the remaining four bits are used to select one of the 16 values (4-bit values) in the selected row, and the selected 4-bit value is output. According to the Kim patent conditions are checked to determine if S-boxes satisfy conditions required for differential and linear cryptanalysis. The Kim patent does not describe, teach, or suggest an S-box formed of a composite function composed of two functions of different algebraic structures.

The cited Langford reference discloses differential-linear cryptanalysis. However, this reference does not describe or suggest an evaluation of resistance of an S-box function against differential-linear cryptanalysis.

The remaining cited references describe established secondary aspects generally related to the field of the invention. However, they fail to complement the primary reference to Kim so as to form a *prima facie* case of obviousness.

In summary, the remaining claims of the application are believed to avoid further rejection under 35 U.S.C. §102 and 103.

In view of the above, consideration and allowance are, therefore, respectfully solicited.

In the event the Examiner believes an interview might serve to advance the prosecution of this application in any way, the undersigned attorney is available at the telephone number noted below.

The Director is hereby authorized to charge any fees, or credit any overpayment, associated with this communication, including any extension fees, to CBLH Deposit Account No. 22-0185, under Order No. 20162-00547-US from which the undersigned is authorized to draw.

Dated: August 5, 2005

Respectfully submitted,

By _____
Morris Liss
Registration No.: 24,510
CONNOLLY BOVE LODGE & HUTZ LLP
1990 M Street, N.W., Suite 800
Washington, DC 20036-3425
(202) 331-7111
(202) 293-6229 (Fax)
Attorney for Applicant